EXPRESS MAIL LABEL NO. EL 842274064 US

PATENT
Docket No. 9437.15

UNITED STATES PATENT APPLICATION

of

RICK V. MURAKAMI

CLARK T. HINTON

and

MATTHEW W. PETTIT

for

METHOD FOR BIOMETRIC AUTHENTICATION THROUGH LAYERING BIOMETRIC TRAITS

KIRTON & McCONKIE
1800 Eagle Gate Tower
60 East South Temple
Salt Lake City, UT 84111-1004
(801) 328-3600

BACKGROUND

Related Application

This application claims priority to the United States Provisional Application filed June 8, 2000, titled "METHOD AND APPARATUS FOR HISTOLOGICAL AND PHYSIOLOGICAL BIOMETRIC OPERATION AND AUTHENTICATION."

Field of the Invention

The present invention relates to a method for electronically authenticating the identity of an individual using the individual's physiological traits. More specifically, the present invention relates to methods for layering a plurality of biometric markers to provide a composite biometric marker for use in authenticating a person's identity.

Background Art

Biometric markers are becoming increasingly more important in today's electronic society. A biometric marker is a biological trait or combination of traits in an individual that is used to authenticate that individual's identity, thereby authorizing a transaction, activating a device, or otherwise instigating some action. In effect, biometric markers are physiological keys or passwords used to authenticate a person's identity to authorize some specific action. Known biometric markers include fingerprints, hand and face geometry, and retinal and iris patterns. Biometric markers also encompass unique behavioral responses such as the recognition of vocal patterns and the analysis of hand movements.

Biometric authentication involves two basic steps: registration and verification. Registration concerns the initial enrollment of a person or individual with the authenticating entity. The individual's biometric information is captured and stored in the form of a biometric template or profile that serves as that individual's identifier. The step of verification involves the subsequent measuring of that individual's biometric information with the stored biometric profile. Authentication of that individual's identity takes place if the newly measured biometric information matches with that in the stored profile.

Various devices exist that capture and electronically process biometric markers for registration and verification. Devices that capture superficial anatomical traits (e.g., finger or hand prints, facial geometry, retinal patterns, etc.) often require unwieldy and/or expensive scanners and optical devices that reflect light off of skin or other surfaces and then capture the reflected light in the form of an electronic signal. These devices then compare one or more features from the signal with a previously stored signal used as an identifier for a particular person. Various features of the signal may be used for the comparison, including a visual representation of a physiological surface produced by the signal; the wave length characteristics of the signal; or the signal characteristics when transformed into a function of the movement of a finger across an optical scanning surface.

In the case of a fingerprint, some devices scan the surface ridges of a fingerprint to form an image representative of the skin print for comparison with a stored image. In the case of a retinal scan, some devices scan a person's retina to form an electronic version of the retina's unique blood vessel pattern. Some devices scan a person's iris to capture its unique

contrasting patterns. Hand and face identification systems use scanners to detect the relative anatomical structure and geometry of a person's face or hand.

Other types of devices capture an individual's behavioral traits such as a signature or voice pattern. Voice recognition systems generally use a telephone or microphone to record a standard phrase repeated by the person to be authenticated; the measured voice pattern is compared to a voice pattern stored in the system. Signature authentication typically involves not only the recording of a pattern of contact between a writing utensil and the recording device, but also the measurement of and comparison between the speed of the writing and the pressure applied while writing.

Known biometric authentication systems have several disadvantages. As was previously mentioned, fingerprint or facial geometry recognition systems may require expensive or large scanning devices. Retinal scanning systems often require a person to place his or her eye close to or upon a scanning device, exposing that person to potential infection. Voice recognition devices have problems screening out background noise. Signature recognition devices are subject to the inherent variations in an individual's signature.

Another disadvantage of the existing art is that it typically is able to use only those biometric markers that are deemed unique to each individual. These markers thus may have only minute differences and must distinguish subtle differences between individual markers. Measuring and authenticating such patterns in turn requires a high degree of electronic sophistication. If the biometric marker is used to identify an individual from among a large

group of individuals, computer memory storage and processing capability may also have to be sophisticated and thus expensive.

An additional disadvantage of prior art is that with relatively few truly unique biometric markers, the likelihood of decreased privacy increases with the widespread use of those markers. In other words, the widespread use of just one or two types of markers increases the likelihood that an unauthorized person could, by chance or otherwise, be improperly granted access. If an unauthorized person were improperly given access, that individual may have access to numerous secured devices or accounts. This is the same problem that exists when a person chooses the same password for all his accounts or electronic devices and the password is stolen.

SUMMARY AND OBJECTS OF THE INVENTION

The present invention provides a biometric authentication system that uses a single technology to measure multiple, varied biological traits to provide authentication based on a combination of biological traits. Preferably, at least one of these biometric markers is an internal, live physiological trait such as a heartbeat waveform. At least one of these biometric traits is a live physiological trait, such as a heartbeat waveform, that is substantially–but not necessarily completely–unique to the population of individuals. Preferably, at least one of the identifying aspects of the biological traits is derived from a measurement taken by reflecting light off of the subdermal layers of skin tissue.

In the preferred embodiments of the present invention, at least one of the biological traits is converted into a digital signal that is normalized to enhance the trait's capacity to function as a biometric marker or identifier. Also, in the preferred embodiments, the biometric authentication system is designed to operate on a portable device such as a PDA or cell phone.

Accordingly, it is an object of some embodiments of the present invention to provide a biometric authentication system using a layered live biometric marker.

It is another object of some embodiments of the present invention to provide a biometric authentication system that greatly increases the possible number of viable biometric identifiers.

It is a further object of some embodiments of the present invention to provide a biometric authentication system that does not require the use of a biometric marker that is completely unique to each individual.

It is a further object of some embodiments of the present invention to provide a layered biometric authentication system that uses a single technology to measure multiple, varied biological traits and is relatively inexpensive and portable.

It is yet another object of some embodiments of the present invention to provide a layered biometric authentication system that does not exclusively rely on the measurement of superficial anatomical structure.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing and other objects and features of the present invention will become more fully apparent from the accompanying drawings when considered in conjunction with the following description and appended claims. Although the drawings depict only typical embodiments of the invention and are thus not to be deemed limiting of the invention's scope, the accompanying drawings help explain the invention in added detail.

Figure 1 illustrates a heartbeat waveform that can serve as one of the biological traits used in the biometric authentication system of the present invention;

Figure 2 illustrates an example of how a heartbeat waveform may be digitally signal processed for use in some embodiments of the present invention; and

Figure 3 shows a diagram of one possible device that may be used in the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The figures listed above are expressly incorporated as part of this detailed description.

It is emphasized that the present invention, as illustrated in the figures and description herein, can be embodied or performed in a wide variety of ways. Thus, neither the drawings nor the following more detailed description of the various embodiments of the system and method of the present invention limit the scope of the invention. The drawings and detailed description are merely representative of the particular embodiments of the invention; the substantive scope of the present invention is limited only by the appended claims.

The various embodiments of the invention will be best understood by reference to the drawings, wherein like elements are designated by like alphanumeric characters throughout. Moreover, it should be noted that because the present invention is computer-implemented, particular embodiments may range from computer executable instructions as part of computer readable media to hardware used to implement the processes herein described. Embodiments of the present invention also include combinations of hardware and computer executable instructions.

Further, whether the invention is described in terms of a method, a system, an application, a type of software, or as computer readable media having computer executable instructions stored thereon, the description is intended to include "instructions" such as program modules, routines, programs, objects, components, data structures, etc. that perform particular tasks within a computing environment. Executable instructions may comprise

instructions and data which cause a general purpose computer, special purpose computer, or special purpose processing device to perform a certain function or group of functions.

In addition, computer readable media may comprise any available media which can be accessed by a general purpose or special purpose computer. By way of example and not limitation, such computer readable media includes any type of RAM (SDRAM, ESDRAM, etc.) or ROM (EPROM, EEPROM, FEPROM, EAROM, etc.) stored on any physical medium, including a computer chip, a server, or a disk. Disks can include optical storage devices (e.g., CD-ROMs or DVD-ROMs), magnetic storage devices (e.g., floppy disks, Zip® disks, or Bernoulli® cartridges), or any other medium that can be used to store the desired executable instructions or data fields and which can be accessed by a general purpose or special purpose computer. Combinations of any of the above-named media are also included within the scope of computer readable media.

The present invention provides a biometric authentication system that uses a single technology to measure multiple, varied biological or histological traits. At least one of the biological traits is a trait that is substantially unique–but not necessarily inherently totally unique (e.g., as in the way that a fingerprint is inherently completely unique to each individual)–to the population of individuals. Although the latter biological trait, herein sometimes referred to as a "first" biological trait, need not be an inherently unique identifier, the latter biological trait is preferably chosen so as to be one that generally remains relatively consistent over time.

In the preferred embodiments of the present invention, a first biological trait is a live physiological trait such as a heartbeat such as that shown in Figure 1. Preferably, the

heartbeat is measured so that various features of the waveform can be used to identify the individual whose waveform is being analyzed. For example, the position on the upslope of the heartbeat waveform having the fastest rate of change slope can be recorded and various attributes of that position can be noted. The amplitude of that position, its position from the center of the pulse and amplitude of the actual beat relative to the position can all be measured and recorded. Thus, multiple quantitative features can be extracted from a single characteristic of a waveform.

The heartbeat waveform can also be analyzed relative to the major peaks such as the two peaks shown in Figure 1. Various parameters associated with waveform peaks include, but are not limited to, the differences between the two peak amplitudes, the differences between the two peak rate of changes, the relative position of the dicrotic notch, how deep the notch is, how far the dicrotic notch is from a zero point or from a reference point, and how far the dicrotic notch is from the center of one of the peaks, where the peak of the dicrotic notch is located along the horizontal, and the position of the various peaks from the center of the waveform and from the center of the other peak.

In the preferred embodiments of the present invention, at least one of the biological traits is converted into a digital signal that is signal processed to enhance the trait's capacity to function as a biometric marker or identifier. For example, in the case of a heartbeat waveform, the captured waveform may be filtered and normalized as shown in Figure 2. In some embodiments of the present invention, some of the quantitative features are globally weighted more than others during normalization and authentication. For example, a particular feature, such as the slope of the dicrotic notch, may be considered more or less

reliable as an identifier and thereby may be given more or less "statistical" weight. Likewise, the correlation between two measurements for a particular feature or the correlation between two different features may be stronger than for other features and be weighted accordingly.

The present invention also employs at least a second biological trait that is used in conjunction with the first biological trait (note: the terms "first" and "second" do not necessarily refer to a chronological order) to provide the biometric authentication of the present invention. This second trait is preferably also a live physiological trait–i.e., a trait measurable only on a living individual (e.g., a fingerprint is not a live trait since it can be measured from a dead individual or tissue)–that is substantially unique to that individual.

Examples of live, potentially substantially unique biological traits include the depth of the various layers of epithelial tissue from a given point on an individual's skin surface. The density of a particular kind of connective tissue, such as bone density, may be another substantially unique histological trait. Likewise, the light absorption characteristics of skin tissue or the visual retinal patterns of an iris could be substantially unique histological traits.

It should be noted that biometric or physiological traits could relate to various physiological systems including the following: the integumentary system, the skeletal system, the muscular system, the pulmonary system, the respiratory system, the circulatory system, the sensory system, the nervous system, the digestive system, the urinary system, the endocrine system, and/or the reproductive system. The physiological traits can be those physiological activities that are both volitional and non-volitional.

Further, the biological traits may be measured and analyzed in a variety of ways. For example, the traits may be measured in terms of spacial measurements such as length, area, and volume. The frequency may be used from a waveform representative of a biological trait. The relative motion of particles and fluids can be measured in terms of velocity, acceleration, volumetric flow rate or angular velocity, and angular acceleration. Physical interaction such as force, surface tension, pressure, viscosity, work, and torque are other possible measurements.

The physiological and histological traits may also be based upon energy or heat related characteristics such as power, heat quantity, heat flux, volumetric heat release, heat transfer coefficient, heat capacity, and thermal conductivity. Likewise, measurements, such as electric quantity, electromotive force, electric field strength, electric resistance, and electrical capacities, could serve as measurements of biometric traits, depending upon the tissue or physiological process being monitored. Characteristics related to magnetism, such as magnetic flux, induce, magnetic permeability, magnetic flux density, magnetic field strength, and magneto-motive force may be used. Other potential measurements may include luminous flux, luminance, illumination, radio nucleotide activity, radioactivity, temperature, and absorbed dose and dose equivalent, and an amount of substance (mole).

In the preferred embodiments of the present invention, the biometric authentication system is designed to operate on a portable computerized device such as a PDA or cell phone. Figure 3 shows an embodiment of the present invention wherein a portable device includes a single computer chip operably connected to a light emitter and detector. In this embodiment, an infrared light (IR) transmitter transmits an IR signal into a person's finger

when the finger is placed on the transmitter (whether for purposes of enrollment or verification). The signal transmitter is activated and a signal is emitted from the signal transmitter and is transmitted into the dermal and subdermal tissues of the person's finger. The signal is partly absorbed and reflected by the dermal and subdermal tissues. The reflected signal is received by a signal receiver and transmitted through receiving wires to a chip where the received signal is processed.

In some embodiments, during the enrollment process, it is preferable if the heartbeat signal captured is the first full heartbeat that occurs after the user has placed his finger on a device. The process preferably takes one second or less. In one embodiment, the biometric measuring hardware is primarily an analog circuitry and takes about one-half second before it is ready to begin sampling a user's heartbeat. Because of hardware limitations in some embodiments, heartbeat signal capture within two or more heartbeats is preferable.

Another biological trait is captured in conjunction (whether simultaneously or subsequently) with the first biological trait. For example, in the case of the first trait being a heartbeat waveform measurement taken by using an IR signal that is reflected off of skin tissue, a convenient second biological trait might be the measurement of the skin's conductance of light. In the preferred embodiments, at least one of the identifying aspects of the biological traits is derived from a measurement taken by reflecting light off of the subdermal layers of skin tissue.

After at least two biological traits are measured, the present invention compares each of the traits to corresponding traits previously enrolled for that individual. If both of

those traits match their respective enrolled traits, then the individual in question is authenticated.

In some embodiments of the present invention, an individual is authenticated when the individual selects a user name or identification that is associated with a particular biological trait such as a normalized waveform. In other words, the biometric traits may be used in conjunction with non-biometric security features such as passwords, social security numbers, ID cards, etc. For example, the individual or user might activate a portable device of the present invention. The device then could prompt the user to select from among several registered users, or ask the user to identify himself or herself. The user may then enter or select some form of identification recognizable to the device, such as a name, social security number or password, and the device would recall from machine memory a previously enrolled normalized waveform associated with the identifying entry/selection. The machine might then measure the user's waveform and compare it with the enrolled waveform recalled from memory. The user is authenticated if the waveforms correspond appropriately.

In some embodiments of the present invention, the authenticating device is designed to provide access to a set number of authorized users. The authorized users would each enroll their individual biometric traits to be stored in a database either inside the portable device or in a remote database that the portable device can access. When a user desires to be authenticated by the portable device, the device scans the trait database and compares the user's presently read trait with the enrolled traits to find a match. If there is a match, the user is granted access.

Some systems of the present invention include means for verifying physiological activity. These means for verifying physiological activity are primarily to prevent an unauthorized person from using dead tissues as a way to circumvent the authentication process. For example, one device involves a personal biometric authentication system wherein inherently specific biometric parameters are measured and recognized and at least one non-specific biometric parameter is recognized and compared with physiological norms. Likewise, one device involves an anti-fraud biometric scanner that determines whether blood flow is taking place in the object being scanned and whether such blood flow is consistent with that of a living human. In addition, some embodiments of the present invention can keep track of a history showing who has accessed the authentication device.

The methods of the present invention are carried out at least in part by machine-readable instructions implemented within a computer-based system. The machine-readable instructions may be located upon any appropriate medium. For example, the instructions may be integrated into a chip or may be stored as data on a portable storage medium such as a floppy disk or CD ROM. The methods of the present invention may likewise be carried out using a signal transmitted over a wired or wireless network wherein the signal carries the machine-readable instructions.

The present invention may be embodied in other specific forms without departing from its spirit or essential characteristics. The described embodiments herein should be deemed only as illustrative. Indeed, the appended claims indicate the scope of the invention; the description, being used for illustrative purposes, does not limit the scope of the

invention. All variations that come within the meaning and range of equivalency of the claims are to be embraced within their scope.

What is claimed is: